




Antitrust Notice

The **Casualty Actuarial Society** is committed to adhering strictly to the letter and spirit of the antitrust laws. Seminars conducted under the auspices of the CAS are designed solely to provide a forum for the expression of various points of view on topics described in the programs or agendas for such meetings.

Under no circumstances shall CAS seminars be used as a means for competing companies or firms to reach any understanding – expressed or implied – that restricts competition or in any way impairs the ability of members to exercise independent business judgment regarding matters affecting competition.

It is the responsibility of all seminar participants to be aware of antitrust regulations, to prevent any written or verbal discussions that appear to violate these laws, and to adhere in every respect to the CAS antitrust compliance policy.

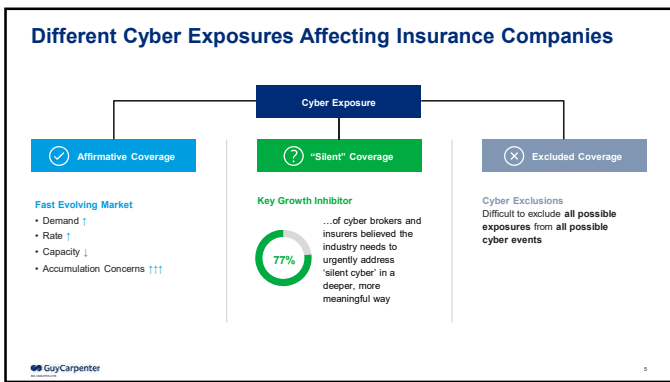


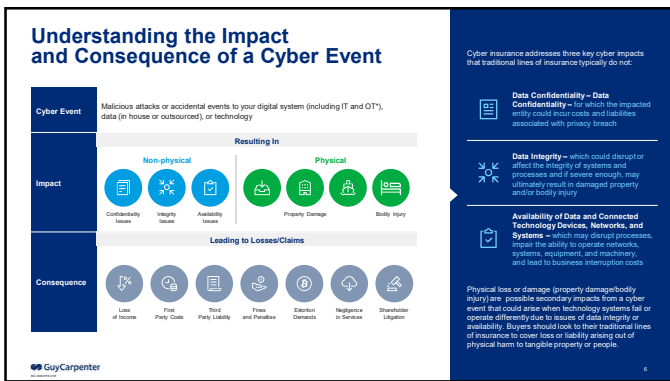
GuyCarpenter

- Introduction to Cyber Insurance Product
- Evolution of Cyber Insurance Market
- Individual Risk Assessment
- Quantifying Cyber Portfolio Risk
- Cyber Catastrophe Considerations

Agenda

Introduction of Cyber Insurance Product





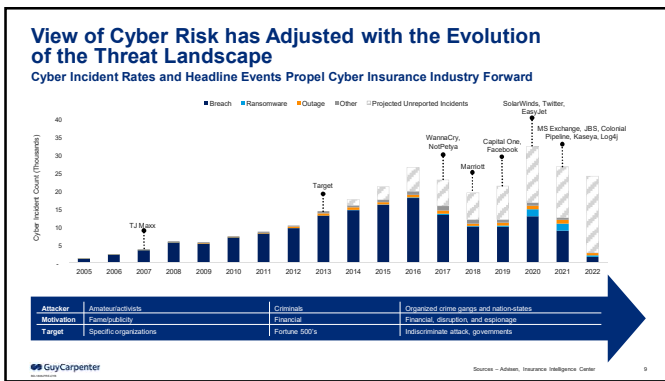
Cyber Risk Scenarios To Consider

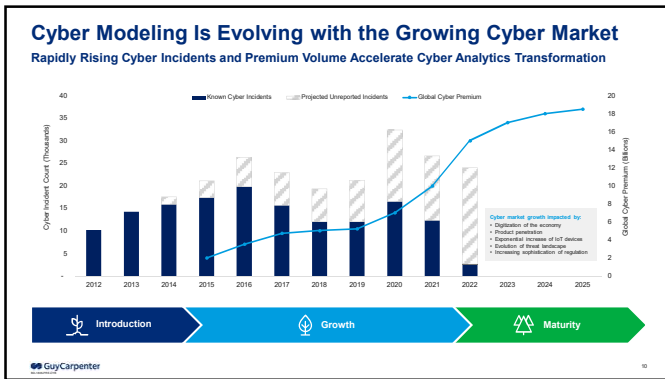
The Potential Impact of Cyber Exclusions to Traditional Policies

	Cyber Event and Primary Impact	Cyber Policy	Secondary Impact	Traditional Policy with a Cyber Exclusion
Property	Malware attack encrypts the data on an automated machine line shutting down production...	Covers IT forensics, business interruption, data restoration and extra expenses	...if corrupted data causes the machinery to overheat and catch fire.	...the fire causes damage to covered tangible property and Business Interruption/Extra Expenses. Covered or excluded?
Marine Liability	A scheduled software update to the navigation system has bad code causing the system to go offline...	With System Failure coverage – covers business interruption (if any), IT forensics, data restoration	...because the navigation is offline, the vessel founders and sinks...	...and the vessel owner is sued for damaged cargo and incurs workers compensation for the injured crew members. Covered or excluded?
General Liability	A high-rise office building sustains a cyber-attack that causes the elevators to go offline, and necessitates the building be temporarily closed...	Covers IT forensics, business interruption, data restoration and extra expenses of the building owner	...a visitor to the building has a heart attack and dies while trapped in the elevator...	...the building owner is sued by the family of dead visitor. Covered or excluded?
Directors and Officers	A publicly traded company experiences a data breach...	Covers breach response, crisis management costs and any privacy or network security liability	...the company sustains a stock drop...	...and a securities class action lawsuit follows. Covered or excluded?

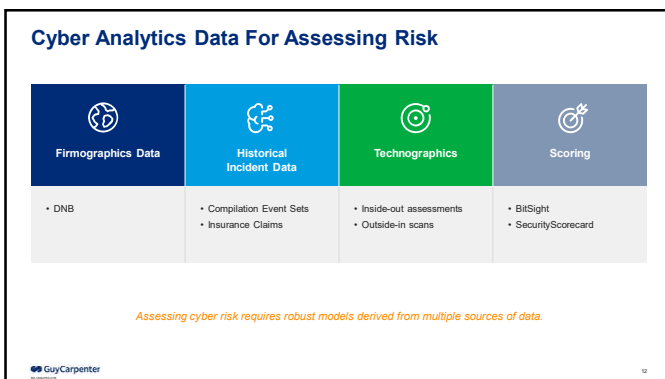
GuyCarpenter Note – These examples are illustrative only. Refer to the actual policies to determine cover.



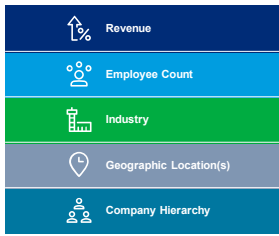








Firmographics



- Company risk highly correlated with revenue and industry
- Sourcing firmographic information
 - Individual risks
- Simple to obtain directly from company
 - Portfolio level
 - Difficult to ensure quality data
 - Revenue and employee count data often modeled
- Complex hierarchies could give misleading results
 - Different business units might need to be modeled separately

Historical Incident Data



Compilation Event Data Sets

- Compiled from public sources, web scraping, FOI requests
- Advantages
 - Broader, more events

- Disadvantages
 - Biased towards larger, US companies
 - Time lag between reporting an event and being added to database



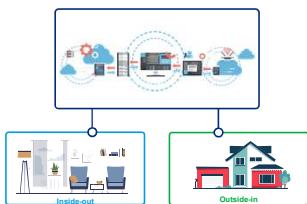
Insurance Claims

- Advantages
 - More detailed, complete

- Disadvantages
 - Limited to companies in your portfolio

Combining multiple sources of incident data can correct for the biases and disadvantages in each.

Technographics



Inside-out Data

- Carrier applications and self-assessments
 - Companies incentivized to be honest
 - Companies might not fully know respond to the questionnaire
- Software or hardware devices installed company networks



Outside-in Data

- Network of sensors that unobtrusively collect data
- Advantages
 - Does not require company input
- Disadvantages
 - Difficult to scale foot printing process while ensuring highly accurate footprints

Scoring and Threat Intelligence

- Turning raw outside-in data into **risk assessments**
- How to utilize these scores
 - Companies can identify areas to **improve their cyber security defenses**
 - Insurance carriers can **gain insight** into the risk an individual company represents
 - Brokers can understand how their clients will be perceived in the **cyber insurance marketplace**
 - Cyber modelers can correlate scores with **incident data or self-assessment questions**
- **Score caveats**
 - Ensure the footprint is **accurate**
 - Don't rely solely or primarily on the **headline score**

500 650 775 850
High Risk Low Risk
640

GuyCarpenter 16

Assessing Cyber Risk

Loss Modeling for Individual Risks

- Scenario Models
- Probabilistic Models
- By Cyber Peril

Exceedance Probability (EP) Curve - Aggregate

10% 9% 8% 7% 6% 5% 4% 3% 2% 1% 0%
0 50 100 150 200 250 300 350 400
Loss Amount (\$ millions)

Loss Amount by Return Period
10 20 50 100 250 500 1,000

GuyCarpenter 17

Assessing Cyber Risk

Correlating Claims With Cyber Self-Assessment Responses

- 1 The organization installs and regularly updates anti-malware solutions on endpoints, servers, and mobile devices
- 2 The organization configures firewalls to prevent unauthorized access
- 3 Our formal firewall policy is to deny-all by default, permit-by-exception
- 4 We review system accounts at least annually and disable any account that cannot be associated with a valid business process and owner
- 5 The organization enforces detailed audit logging of access or changes to sensitive data

GuyCarpenter 18

Key Takeaways



Company firmographics influence baseline risk



Risk can be altered depending on an organization's cyber security defenses

- Use technographics and scoring data to gain insight

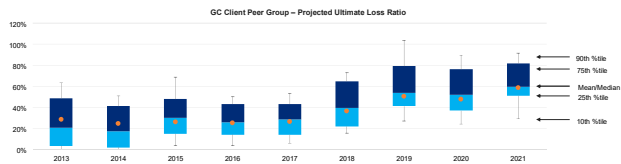


Using multiple types of data from multiple sources can correct for the biases in each

Quantifying Cyber Portfolio Risk



Global Cyber Industry Performance



- GC tracks peer-group cyber performance based on a diverse mix of ~40 cyber client portfolios
- Results vary by year due to carriers' underlying composition of business, limits, and attachment points
- LLR post-2018 represents the new normal in the industry with many factors at play: rate, loss emergence, trend
- Differentiating experience by year is critical as carriers weigh recent years' performance more heavily than pre-2019

Rate Environment Signaling Stabilization

Global Cyber Market Update – Q2 2022

US Cyber Clients – All Industries

Marsh US Cyber Composite Pricing Change

UK Cyber Clients – All Industries

Cyber Price Change – All Industries

Rate Environment Observations

- Rate increases for 2022 are expected to be heavier in Q1/Q2 than in Q3/Q4 due to the accelerated rate curve in Q3 2021
- Pricing increases continue to show signs of stabilization in Q2 22 to 78.8% from the Q4 '21 high of 139.4% for the same quarter year prior in the US
- Similarly for the UK, rates have slowed to 98% in Q2 22
- Insurers focusing on re-evaluation rating models and adequate pricing on new and renewal business
- Fluctuations in rate may reemerge as the threat landscape evolves

Beyond Rate Considerations

- Anticipated rate increases, frequency and severity of losses have resulted in a reduction of capacity at large in the primary market
- Collecting the right data and integrating risk insights into underwriting methodology and T&Cs
- Managing limit deployments, sublimits, and risk selection
- Shoppers: lower paid ransom demands in the portfolio when policyholders are better prepared

Source – Marsh Global Placement & Specialist, Data and Analytics, PhasIDP

Deriving Cyber Loss Development Pattern Actuarially

Loss Development Pattern (% to Ultimate)

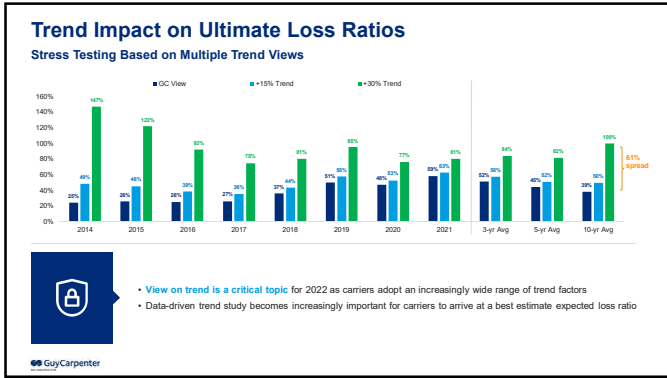
- As more cyber claims data becomes available, actuarial techniques can be used to derive credible and stable loss development patterns
- Empirical data indicates ransomware claims develop faster than all other cyber claims, and cyber has shorter development than traditional long-tail PL lines

Estimating Cyber Loss Trend Using Actuarial Methods

- Study based on proprietary GC data of ~40 global portfolios ranging from mid-size regional carriers to large global carriers
- Modelling frequency and severity trends separately were considered, but yielded no discernible trends given the volatility observed in the data
- Future enhancements to trend study:
 - Continue to monitor frequency and severity trends separately
 - As data becomes more credible, consideration to model trends separately by coverage (1st party vs 3rd party) and claim type (Ransomware vs other claims)

On-Level Ultimate Loss Ratio

	Linear Trend	Exponential Trend	GC Selection
2017 and Prior	+1.3%	+1.5%	+1.5%
2018 and Subsequent	+9.7%	+12.7%	+11.0%



Key Takeaways

Traditional actuarial techniques can be applied to cyber claims data, given the increase volume of credible information to-date

However, the potential of cyber cat losses cannot be contemplated based on actual cyber loss experience

- Cyber cat events are few and far between in the past
- Most of them did not result in significant insured loss
- Potential understatement of silent cyber loss, due to carriers' inability to link non-cyber claims with cyber trigger

GuyCarpenter

Cyber Catastrophe Considerations

Cyber Events by Scope of Impact

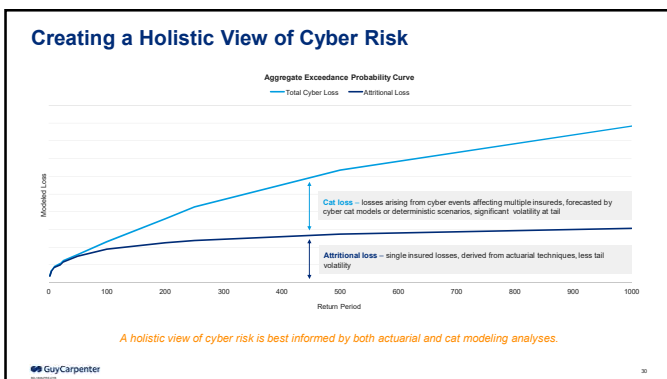
Single Risk		Additional Cyber Loss
<ul style="list-style-type: none"> NFT as attack vector Manufacturing compromise (JBS) 	<ul style="list-style-type: none"> Airport/Dam/Rail control system disruption Deepwater Horizon 	
Limited Affected Companies		Systemic
<ul style="list-style-type: none"> Marine navigation/port/freight transport disruption Medical records corruption Hospital network disruption Precision agriculture Induced earthquake Satellite disruption 	<ul style="list-style-type: none"> Industrial Control Systems failure High wind alert/Tsunami warning center failure Airplane software disruption Water utility systems disruption Hack on centralized ledger systems Infiltration of password wallet 	
		<ul style="list-style-type: none"> Financial meltdown Ransomware contagion Katereya Cloud cascade Cyber-triggered pandemic All attack

GuyCarpenter 28

Systemic Cyber Cat's Aggregation Point Concept

CyberCube	Cyence
<p>Single-point-of-failure (SPoF) as possible cyber targets associated with each scenario in the model</p> <ul style="list-style-type: none"> CyberCube collects raw data feeds from multiple third-party vendors to build their technology mapping database SPoF intelligence feature different reflects types of revenue reliance e.g., SaaS, PaaS, IaaS Additional capability to create a custom view into non-modeled SPoF risk 	<p>Accumulation paths represent risks common to multiple companies based on the usage of shared technologies</p> <ul style="list-style-type: none"> Technological information of companies collected through Cyence's data listening engine The following event types are modeled, each consisting of unique accumulation paths representing a specific technology: <ul style="list-style-type: none"> Service provider outage Software zero-day vulnerability Payment processor outage Ransomware

GuyCarpenter 29





Guy Carpenter & Company, LLC provides this report for general information only. The information contained herein is based on sources we believe reliable, but we do not guarantee its accuracy, and it should be understood to be general information only. Guy Carpenter & Company, LLC makes no representation or warranty, express or implied. The information is not intended to be used as advice with respect to any financial decision and cannot be relied upon in such. Statements concerning tax, accounting, legal or regulatory matters should be understood to be general observations based solely on our experience as insurance brokers and risk consultants, and may not be relied upon as tax, accounting, legal or regulatory advice, which we are not licensed to provide. All such topics should be reviewed with your qualified advisors in these areas.

Readers are cautioned not to place undue reliance on any historical, current or forward-looking statements. Any such predictions are subject to inherent risks and uncertainties. Any forward-looking statements may depend on assumptions made, or risks or uncertainties that may be realized, economic, regulatory, business and other conditions in addition. Guy Carpenter & Company, LLC declines its responsibility for actual results in each year. Guy Carpenter & Company, LLC disclaims its obligation to update or revise publicly any historical, current or forward-looking statements, whether as a result of new information, research, future events or otherwise. All decisions in connection with any matter contained in this report are the sole responsibility of the recipient. The forecasts and other results contained herein are the property of their respective sources.

©2022 Guy Carpenter & Company, LLC. All rights reserved.

A business of Marsh McLennan

Copyright © 2022 Guy Carpenter & Company, LLC. All rights reserved.
